# IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

SEPRACOR, INC.,	)
Plaintiff, Counterclaim-Defendant	) ) C.A. No. 06-113-***(MPT) ) (Consolidated)
v.	)
DEY, L.P. and DEY, INC.,	)
Defendants, Counterclaim Plaintiffs.	) ) )

# NOTICE OF DEPOSITION OF SEPRACOR, INC.

PLEASE TAKE NOTICE that at 9:00 a.m. on April 27, 2007, and continuing from day to day until completed, defendants, Dey, L.P. and Dey, Inc., ("Dey"), will take the deposition of Sepracor Inc. ("Sepracor"), whose business address is 84 Waterford Drive, Marlborogh, MA 01752. The deposition will be taken at the offices of Frommer Lawrence & Haug LLP, 745 Fifth Avenue, New York, New York 10151, or at such other location as is mutually agreeable.

In accordance with Rule 30(b)(6) of the Federal Rules of Civil Procedure, Sepracor is advised that it is required to designate one or more officers, directors, managing agents, or other persons who consent to testify on its behalf with respect to the matters set forth in attached Exhibit A. No less than five business days before the scheduled deposition date, Sepracor is requested to designate in writing to Dey the names of the persons who will testify on its behalf, specifying the matters on which each person will testify.

The deposition will be taken in accordance with the Federal Rules of Civil Procedure before an official authorized by law to administer oaths and will continue from day to day until completed. The testimony will be recorded by stenographic and/or videographic means.

You are invited to attend and cross-examine.

# **ASHBY & GEDDES**

/s/ Tiffany Geyer Lydon

Steven J. Balick (I.D. #2114) John G. Day (I.D. #2403) Tiffany Geyer Lydon (I.D. #3950) 500 Delaware Avenue, 8th Floor P.O. Box 1150 Wilmington, Delaware 19899 (302) 654-1888 sbalick@ashby-geddes.com iday@ashby-geddes.com tlydon@ashby-geddes.com

Attorneys for Defendants Dey, L.P. and Dey, Inc.

# Of Counsel:

Edgar H. Haug John S. Goetz FROMMER, LAWRENCE & HAUG L.L.P. 745 Fifth Avenue New York, New York 10151 (212) 588-0800

Elizabeth A. Leff FROMMER, LAWRENCE & HAUG L.L.P. 1667 K Street, N.W. Washington, D.C. 20006 (202) 292-1530

Dated: April 5, 2007

179498.1

### Exhibit A

In accordance with Rule 30(b)(6) of the Federal Rules of Civil Procedure, plaintiff, Sepracor Inc. ("Sepracor"), has a duty to designate one or more officers, directors, managing agents, or other persons who consent to testify on its behalf with respect to the matters set forth below. By April 19, 2007, Sepracor should inform Dey of the person(s) designated to testify on its behalf with respect to these matters and specify the matters on which each person will testify.

#### I. SYSTEM PROFILE

- 1. Sepracor's network architecture and usage policies.
- 2. Types of data processing and data storage devices used by Sepracor in the course of business.
- 3. Number, types, locations and names of computers (including desktops, laptops, PDAs, cell phones, etc.) currently in use by Sepracor, or in use at any time during the past 13 years.
- 4. Number, types, locations, and names of servers currently in use by Sepracor, or in use at any time during the past 13 years.
- 5. Brands and versions of software used on Sepracor's computer system(s).
- 6. Sepracor's file naming and saving conventions.
- 7. Identity of the person(s) responsible for the ongoing operation, maintenance, expansion, backup, and upkeep of Sepracor's computer systems and how frequently these activities occur (according to policy and actual practice).
- 8. Sepracor's policies and practices for usage of home computers for business purposes.
- 9. Sepracor's modification of use of computers since notice of this litigation.
- 10. Utility programs used to permanently "wipe files" from Sepracor's computer(s) and date(s) used since notice of litigation.
- 11. Sepracor's upgrades to computer hardware during the past 13 years.
- 12. Sepracor's upgrades or replacements to computer software during the past 13 years.

#### II. BACKUP AND RETENTION

- 1. Steps Sepracor has taken to ensure preservation of electronic data.
- 2. Deletion of any documents since lawsuit commenced or since Sepracor reasonably anticipated this litigation.
- 3. Sepracor's instructions about preservation of electronic documents due to this lawsuit: Who provided notification? How was it disseminated? When was it disseminated? What procedures were in place for verification of receipt?
- 4. Sepracor's backup software program(s) (e.g., ARCserve, Backup Exec, StorageExpress, Legato, Veritas, etc.).
- 5. Any modification of Sepracor's backup procedures since notice of litigation.
- 6. Information about Sepracor's disaster recovery plans in place currently and during past 13 years.
- 7. Sepracor's backup tape or archival disk naming/labeling conventions.
- 8. The current location, identification, and status of Sepracor's backup tapes and other backup media.
- 9. Method and schedule Sepracor uses to delete files from its computer system(s).
- 10. Location(s), if any, where Sepracor files are "archived" off the system.
- 11. Dates, if any, when Sepracor data was restored from backup tapes within the past 48 months. If so: What data was restored? Why was the data restored?

## III. POLICIES AND PROCEDURES

- 1. Sepracor's electronic records management policies and procedures.
- 2. Sepracor's policy regarding purging of individual directories when an employee leaves the company (on desktop, laptop, and server systems).
- 3. Sepracor's policy regarding reassigning workstations to incoming employees.
- 4. Sepracor's policy regarding disposal/recycling/sale of hardware.
- 5. Sepracor's procedures for handling used disks or drives before destruction or sale.
- 6. Sepracor's policy and procedure for use of outside contractors to upgrade either hardware or software for system maintenance.

- 7. Sepracor's protocol for using passwords or encrypted files are used on any of the computer systems, including name(s) of person(s) who manage this process.
- 8. Sepracor's policy for changing/revoking passwords and access codes when an employee leaves the company.
- 9. Sepracor's method used for those outside the company to access the computers (VPN or other).

#### IV. DATABASES

- 1. Types of databases Sepracor uses (CRM, accounting, etc.).
- 2. Type(s) and names of database software Sepracor uses (e.g., Oracle, dBASE, Advanced Revelation, Access, proprietary, etc.).
- 3. The fields of information used in Sepracor's database(s).
- 4. Identity of person(s) responsible for Sepracor's database design, database maintenance, report design, database backup.
- 5. Identity of person(s) who enter information into the Sepracor's database(s).
- 6. Ways and by whom the Sepracor's databases are accessed.
- 7. Identification of any standard reports prepared on a routine basis.
- 8. Incidents and dates on which Sepracor's database files have been re-indexed, purged, repaired, or archived.

#### IV. SHARED FILES

- 1. Types of shared files Sepracor uses.
- 2. Type(s) and names of shared file software Sepracor uses.
- 3. Identity of person(s) responsible for Sepracor's shared files directory design, shared files maintenance, and shared files backup.
- 4. Ways and by whom the Sepracor's shared files are accessed.
- 5. Incidents and dates on which Sepracor's shared files have been re-indexed, purged, repaired, or archived.
- 6. Sepracor's shared file directory structure.
- 7. Sepracor's shared file naming and saving conventions.

#### V. EMAIL SYSTEMS

- 1. Identity of person(s) responsible for administering Sepracor's email system(s).
- 2. Identification of all type(s) of email programs currently in use by Sepracor, including name(s) and version number(s), installation date(s), and number of users.
- 3. Location of Sepracor users' email files (e.g., mail messages stored in a central location—a server—or locally on users' desktops, or both?).
- 4. Ways, if any, Sepracor users can access their email remotely (e.g., from outside the office via BlackBerry or other wireless device, or via a web mail application).
- 5. Sepracor's protocol for routinely changing email passwords.
- 6. Sepracor's policy for running "janitorial" programs to purge email.
- 7. Identification of any other Sepracor email systems used in the past 13 years.
- 8. Details about Sepracor's email retention policies and practices (e.g., retention period, auto-delete features, deletion procedures, etc.)
- 9. Restoration of any mailboxes from Sepracor backup tapes within the past 48 months/years. If applicable, identify: What mailbox(es) was/were restored? Was the restoration operation successful? What resources were required to perform the restoration (labor hours, equipment, drive space, etc.).
- 10. Sepracor's special active email retention settings.
- 11. Incidents and dates on which Sepracor's email databases have been re-indexed, purged, repaired, or archived.

#### VI. MISCELLANEOUS

- 1. Information about production of Sepracor electronic documents in other litigation or legal proceedings: Which cases were produced? What was produced, in what format?
- 2. Information about any persons who examined any of Sepracor's computers since learning of this lawsuit, including details about reasons for examination and protocol utilized.
- 3. The list of Sepracor's backup electronic systems provided to Dey on October 3, 2006.
- 4. The current location, identification, and status of backup electronic media for Sepracor's First Class email system.

- 5. All stored data from Sepracor's First Class email system.
- 6. Sepracor's 1999 move of email from the First Class system to the Microsoft Exchange server.
- 7. Sepracor's backup cartridge made in April 1999, a photocopy of which was attached to Sepracor's March 19, 2007 letter to Dey.